



CHAPTER 33

Configuring Certificates

Digital certificates provide digital identification for authentication. A digital certificate contains information that identifies a device or user, such as the name, serial number, company, department, or IP address. CAs issue digital certificates in the context of a PKI, which uses public-key/private-key encryption to ensure security. CAs are trusted authorities that “sign” certificates to verify their authenticity, thus guaranteeing the identity of the device or user.

For authentication using digital certificates, there must be at least one identity certificate and its issuing CA certificate on a security appliance, which allows for multiple identities, roots and certificate hierarchies. There a number of different types of digital certificates listed below:

- A *CA certificate* is one used to sign other certificates. A CA certificate that is self-signed is called a *root certificate*; one issued by another CA certificate is called a *subordinate certificate*. See [CA Certificate Authentication](#).
- CAs also issue *identity certificates*, which are the certificates for specific systems or hosts. See [Identity Certificates Authentication](#).
- *Code-signer certificates* are special certificates used to create digital signatures to sign code, with the signed code itself revealing the certificate origin. See [Code-Signer Certificates](#)
- The Local Certificate Authority (CA) integrates an independent certificate authority functionality on the security appliance, deploys certificates, and provides secure revocation checking of issued certificates. The Local CA provides a secure configurable inhouse authority for certificate authentication with user enrollment by browser web page login. See [Local Certificate Authority](#), [Manage User Certificates](#), and [Manage User Database](#).

CA Certificate Authentication

The CA Certificates panel allows you to authenticate self-signed or subordinate CA certificates and to install them on the security appliance. You can create a new certificate configuration or you can edit an existing one.

If the certificate you select is configured for manual enrollment, you should obtain the CA certificate manually and import it here. If the certificate you select is configured for automatic enrollment, the security appliance uses the SCEP protocol to contact the CA, and then automatically obtains and installs the certificate.

CA Certificates Fields

- **Certificates** —Displays a list of the certificates available identified by issued to and by, the date the certificate expires, and the certificate’s usage or purpose. You can click a certificate in the list and edit its configuration, or you can add a new certificate to the displayed list.

- **Add Button**—Add a new certificate configuration to the list. See [Add/Install a CA Certificate](#).
- **Edit Button**—Modify an existing certificate configuration. See [Edit CA Certificate Configuration](#).
- **Show Details Button**—Display the details and issuer information for the selected certificate. See [Show CA Certificate Details](#).
- **Request CRL Button**—Access the Certificate Revocation List (CRL) for an existing CA certificate. See [Request CRL](#).
- **Delete Button**—Remove the configuration of an existing CA certificate. See [Delete a CA Certificate](#).
- **Apply Button**—Save the new or modified CA certificate configuration.
- **Reset Button**—Remove any edits and return the display to the original contents.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Add/Install a CA Certificate

The CA Certificate panel lets you add a new certificate configuration from an existing file, by manually pasting a certificate, or by automatic enrollment. Click the appropriate option to activate one of the following:

- **Install from a File:**—To add a certificate configuration from an existing file, enter the path and file name, then click **Install Certificate**. You can type the pathname of the file in the box or you can click **Browse** and search for the file. **Browse** displays the Load CA certificate file dialog box that lets you navigate to the file containing the certificate.
- **Paste certificate in PEM format:**—For manual enrollment, copy and paste the PEM format certificate (base64 or hexadecimal format) into the panel, then click **Install Certificate**.
- **Use SCEP:**—For automatic enrollment, the security appliance contacts the CA using Simple Certificate Enrollment Protocol (SCEP) protocol, obtains the certificates, and installs them on the device. (SCEP). SCEP is a secure messaging protocol that requires minimal user intervention. SCEP lets you to enroll and install certificates using only the VPN Concentrator Manager. To use SCEP, you must enroll with a CA that supports SCEP, and you must enroll via the Internet.

SCEP automatic enrollment requires completion of the following fields:

- **SCEP URL: HTTP://** Enter the path and file name of the certificate to be automatically installed.
- **Retry Period:** Specify the maximum number of minutes to retry installing a certificate. The default is one minute.
- **Retry Count:** Specify the number of retries for installing a certificate. The default is 0, which indicates unlimited retries within the retry period.

More Options... —For additional options for new certificates, click the **More Options...** button to display configuration options for new and existing certificates. See [Configuration Options for CA Certificates](#).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Edit CA Certificate Configuration

To modify the characteristics of an existing certificate, select the certificate and click the **Edit** button to display a number of tab-selectable displays that address CA certificate configuration specifics. For details, see [Configuration Options for CA Certificates](#).

Show CA Certificate Details

The **Show Details** button displays the Certificate Details dialog box, which shows the following information about the selected certificate:

- **General**—Displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated certificates. This applies to both available and pending status.
- **Issued to**—Displays the X.500 fields of the subject DN or certificate owner and their values. This applies only to available status.
- **Issued by**—Displays the X.500 fields of the entity granting the certificate. This applies only to available status.

Request CRL

The **Request CRL** button updates the current version of the Certificate Revocation List (CRL). CRL update provides the current status of certificate users. If the request fails, an error message displays.

The CRL is generated and regenerated automatically until it expires; the **Request CRL** button forces an immediate CRL file update and regeneration.

Delete a CA Certificate

The **Delete** button immediately removes the selected CA Certificate configuration from the security appliance. Once you delete a certificate configuration, it cannot be restored; to recreate the deleted certificate, you must use the **Add** button to reenter the certificate configuration information from the beginning.



Note

Once you delete a certificate configuration, it cannot be restored.

Configuration Options for CA Certificates

Additional configuration options are available, whether you are adding a new CA certificate with the **Add** button or modifying an existing CA certificate with the **Edit** button.

The following panels are the tab-selectable displays that address CA certificate configuration specifics. Each tabbed display is summarized in the following list:

Revocation Check—The Revocation Check panel lets you chose or reject revocation checking, specify a method of revocation checking (CRL or OCSP) and allows you to ignore revocation-checking errors when validating a certificate. For details of the Revocation Check panel, see [Revocation Check Configuration](#).

CRL Retrieval Policy—The CRL Retrieval Policy panel allows you to configure use of the CRL distribution point and/or static CRL URLs, with capabilities to add, edit, and delete status CRL URLs. For details, see [CRL Retrieval Policy Configuration](#).

CRL Retrieval Method—The CRL Retrieval Method panel allows you to chose Lightweight Directory Access Protocol (LDAP), HTTP, or Simple Certificate Enrollment Protocol (SCEP) as the method to be used for CRL retrieval. For the LDAP method, you can configure the LDAP parameters and security. See [CRL Retrieval Method Configuration](#).

OCSP Rules—Online Certificate Status Protocol (OCSP) is used for obtaining revocation status of an X.509 digital certificate and is an alternative to certificate revocation lists (CRL). For details, see OCSP Rules Configuration. Refer to [OCSP Rules Configuration](#).

Advanced—The Advanced panel allows you to set up CRL update parameters, OCSP parameters, and certificate acceptance and validation parameters. See [Advanced Configuration Options](#).

Revocation Check Configuration

With the **Revocation Check** Edit Option panel, you can specify degrees of user certificate revocation checking as follows:

No Revocation Checking - Click the **Do not check certificates for revocation** button to disable revocation checking of certificates.

Revocation Checking Method(s) - Click the **Check certificates for revocation** to select one or more revocation checking methods. Available methods display on the left; use the **Add** button to move a method to the right.

The methods you select are implemented in the order in which you add them. If a method detects an error, subsequent revocation checking methods activate.

Revocation Checking Override - Click the **Consider certificate valid if revocation checking returns errors** button to ignore revocation-checking errors.

CRL Retrieval Policy Configuration

With the CRL Retrieval Policy panel, you specify either the CRL Distribution Point, or a static go-to location for the CRL revocation checking.

- Certificate CRL Distribution Point - Click the **Use CRL Distribution Point from the certificate** button to direct revocation checking to the CRL DP included on the certificate being checked.
- Static URL - Click the **Use Static URLs configured below** button to list specific URLs to be used for CRL Retrieval. The URLs you select are implemented in the order in which you add them. If a specified URL errors, subsequent URLs are accessed in order.

::/—Type the location that distributes the CRLs.

CRL Retrieval Method Configuration

The CRL Retrieval Method panel lets you select the method to be used for CRL retrieval.

- Click the **Enable Lightweight Directory Access Protocol (LDAP)** button to specify LDAP CRL retrieval. With LDAP, CRL retrieval starts an LDAP session by connecting to a named LDAP server, accessed by password. The connection is on TCP port 389 by default. Enter the specific LDAP parameters required:
 - Name:
 - Password:
 - Confirm Password:
 - Default Server: (server name)
 - Default Port: 389 (default)
- HTTP - Click the **Enable HTTP button** to select HTTP CRL retrieval
- SCEP - Click the **Enable Simple Certificate Enrollment Protocol (SCEP)** to select SCEP for CRL retrieval.

OCSP Rules Configuration

The Online Certificate Status Protocol (OCSP) panel lets you configure OCSP rules for obtaining revocation status of an X.509 digital certificate.

OCSP Rules Fields

- **Certificate Map**—Displays the name of the certificate map to match to this OCSP rule. Certificate maps match user permissions to specific fields in a certificate. You must configure the certificate map before you configure OCSP rules.
- **Certificate**—Displays the name of the CA the security appliance uses to validate responder certificates.
- **Index**—Displays the priority number for the rule. The security appliance examines OCSP rules in priority order, and applies the first one that matches.
- **URL**—Specifies the URL for the OCSP server for this certificate.
- **Add**—Click to add a new OCSP rule.
- **Edit**—Click to edit an existing OCSP rule.
- **Delete**—Click to delete an OCSP rule.

Advanced Configuration Options

The **Advanced** tab lets you specify CRL and OCSP options. When a certificate is issued, it is valid for a fixed period of time. Sometimes a CA revokes a certificate before this time period expires; for example, due to security concerns or a change of name or association. CAs periodically issue a signed list of revoked certificates. Enabling revocation checking forces the security appliance to check that the CA has not revoked the certificate being verified.

The security appliance supports two methods of checking revocation status: CRL and OCSP.

Fields

- **CRL Options**
 - **Cache Refresh Time**—Specify the number of minutes between cache refreshes. The default number of minutes is 60. The range is 1-1440.

To avoid having to retrieve the same CRL from a CA repeatedly, The security appliance can store retrieved CRLs locally, which is called CRL caching. The CRL cache capacity varies by platform and is cumulative across all contexts. If an attempt to cache a newly retrieved CRL would exceed its storage limits, the security appliance removes the least recently used CRL until more space becomes available.

- **Enforce next CRL update**—Require valid CRLs to have a Next Update value that has not expired. Clearing the box allows valid CRLs with no Next Update value or a Next Update value that has expired.
- **OCSP Options**
 - **Server URL:**—Enter the URL for the OCSP server. The security appliance uses OCSP servers in the following order:
 1. OCSP URL in a match certificate override rule
 2. OCSP URL configured in this OCSP Options attribute
 3. AIA field of remote user certificate
 - **Disable nonce extension**—By default the OCSP request includes the nonce extension, which cryptographically binds requests with responses to avoid replay attacks. It works by matching the extension in the request to that in the response, ensuring that they are the same. Disable the nonce extension if the OCSP server you are using sends pre-generated responses that do not contain this matching nonce extension.
- **Validation Policy**
 - **Specify the type of client connections that can be validated by this CA**—Click SSL or IPsec to restrict the type of remote session this CA can be used to validate, or click SSL and IPsec to let the CA validate both types of sessions.
- **Other Options**
 - **Accept certificates issued by this CA**—Specify whether or not the security appliance should accept certificates from **CA Name**.
 - **Accept certificates issued by the subordinate CAs of this CA**

Identity Certificates Authentication

An Identity Certificate can be used to authenticate VPN access through the security appliance. Click the *SSL Settings* or the *IPsec Connections* links on the Identity Certificates panel for additional configuration information.

The Identity Certificates Authentication panel allows you to:

- Add an Identity Certificate. See [Add/Install an Identity Certificate](#).
- Display details of an Identity Certificate. See [Show Identity Certificate Details](#).
- Delete an existing Identity Certificate. See [Delete an Identity Certificate](#).
- Export an existing Identity Certificate. See [Export an Identity Certificate](#).
- Install an Identity Certificate. See [Installing Identity Certificates](#).
- Enroll for a certificate with Entrust. See [Generate](#)

Add/Install an Identity Certificate

The Identity Certificate panel lets you import an existing identity certificate from a file or add a new certificate configuration from an existing file.

Click the appropriate option to activate one of the following:

Add Identity Certificate Fields

Assign values to the fields in the **Add Identity Certificate** dialog box as follows:

- To import an identity certificate from an existing file, select **Import the identity certificate from a file** and enter the following information:
 - Decryption Pass Phrase—Specify the passphrase used to decrypt the PKCS12 file.
 - File to Import From—You can type the pathname of the file in the box or you can click **Browse** and search for the file. **Browse** displays the Load Identity Certificate file dialog box that lets you navigate to the file containing the certificate.
- To add a new identity certificate requires the following information:—
 - Key Pair—RSA key pairs are required to enroll for identity certificates. The security appliance supports multiple key pairs.
 - Key Pair name (in Key Pair > Show window)— Specifies name of the key pair whose public key is to be certified.
 - Generation time (in Key Pair > Show window)—Displays time of day and the date when the key pair is generated.
 - Usage (in Key Pair > Show window)— Displays how an RSA key pair is to be used. There are two types of usage for RSA keys: *general purpose* (the default) and *special*. When you select *Special*, the security appliance generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.
 - Modulus Size (bits) (in Key Pair > Show window)— Displays the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
 - Key Data: (in Key Pair > Show window)—Indicates the window that contains the specific key data
 - Name (in Key Pair > New window)—Selects a default key pair name, such as <Default-RSA-Key>, or you can enter a new key pair name.
 - Size (in Key Pair > New window)—Specifies the default key pair size: 512, 788, 1024 (the default) or 2048.
 - Usage (in Key Pair > New window)— Specifies the key pair usage as *general purpose* or *special*.
- The **Advanced** button on the **Add Identity Certificate** pane lets you establish the following certificate parameters, enrollment mode, and an optional revocation password for the device-specific identity certificate:
 - **FQDN** (in Advanced > Certificate Parameters)—The Fully Qualified Domain Name (FQDN), an unambiguous domain name, specifies the position of the node in the DNS tree hierarchy.
 - **E-mail** (in Advanced > Certificate Parameters)— The e-mail address associated with the Identity Certificate.
 - **IP Address** (in Advanced > Certificate Parameters)—The security appliance address on the network in four-part dotted-decimal notation.

- The check box **Include serial number of the device** allows you to add the security appliance serial number to the certificate parameters.
- The Advanced > Enrollment Mode allows you to select either manual enrollment (**Request by manual enrollment**) or enrollment by CA (**Request from a CA**), which requires the following information:
 - **Enrollment URL (SCEP): HTTP://** Enter the path and file name of the certificate to be automatically installed.
 - **Retry Period:** Specify the maximum number of minutes to retry installing an Identity certificate. The default is one minute.
 - **Retry Count:** Specify the number of retries for installing an Identity certificate. The default is 0, which indicates unlimited retries within the retry period.
- In the **Add Identity Certificate** pane, enter the following Certificate Subject DN information:
 - **Certificate Subject DN**— Specify the certificate subject-name DN to form the DN in the Identity certificate, and click the **Select...** button to add DN attributes in the Certificate Subject DN pane.
 - **Attribute:** (in Certificate Subject DN > Select window)— Select one or more DN attributes from the pull-down menu. Selectable X.500 fields of attributes for the Certificate Subject DN are:

Certificate Subject DN Attributes

CN = Common Name
OU = Department
O = Company Name
C = Country
ST = State/Province
L = Location
EA = E-mail Address

- **Value:** (in Certificate Subject DN > Select window)— Enter the value for each of the DN attributes that you select in the **Attribute** list. With a value assigned to an attribute, use the now-active **Add** button to add the attribute to the Attribute/Value field on the right. To remove attributes and their values, select the attribute and click the now-active **Delete** button.

Once you complete Identity Certificate configuration, click **Add Certificate** in the Add Identity Certificate pane. Then, be sure to click the **Apply** button in the **Identity Certificates** window to save the newly certificate configuration.

Show Identity Certificate Details

The **Show Details** button displays the Certificate Details dialog box, which shows the following information about the selected certificate:

- **General**—Displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated certificates. This applies to both available and pending status.

- **Issued to**—Displays the X.500 fields of the subject DN or certificate owner and their values. This applies only to available status.
- **Issued by**—Displays the X.500 fields of the entity granting the certificate. This applies only to available status.

Delete an Identity Certificate

The **Delete** button immediately removes the selected Identity Certificate configuration from the security appliance. Once you delete a certificate configuration, it cannot be restored; to recreate the deleted certificate, use the **Add** button to reenter the certificate configuration information from the beginning



Note Once you delete a certificate configuration, it cannot be restored.

Export an Identity Certificate

The **Export** panel lets you export a certificate configuration with all associated keys and certificates in PKCS12 format, which must be in base64 format. An entire configuration includes the entire chain (root CA certificate, identity certificate, key pair) but not enrollment settings (subject name, FQDN and so on). This feature is commonly used in a failover or load-balancing configuration to replicate certificates across a group of security appliances; for example, remote access clients calling in to a central organization that has several units to service the calls. These units must have equivalent certificate configurations. In this case, an administrator can export a certificate configuration and then import it across the group of security appliances.

Export Identity Certificate Fields

- **Export to a file**—Specify the name of the PKCS12-format file to use in exporting the certificate configuration;
- **Certificate Format**—Click PKCS12 format, the public key cryptography standard, which can be base64 encoded or hexadecimal, or click PEM format.
 - **Browse**—Display the **Select a File** dialog box that lets you navigate to the file to which you want to export the certificate configuration.
- **Encryption Passphrase**—Specify the passphrase used to encrypt the PKCS12 file for export.
 - **Confirm Passphrase**—Verify the encryption passphrase.
- **Export Certificate**—Export the certificate configuration.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Generate Certificate Signing Request

This pane lets you generate a certificate signing request to send to Entrust. Be aware that at the time of this release, Entrust supports key modulus of size 1024 only. Consult Entrust if you are using any other value.

Generate Certificate Signing Request Fields

- **Key Pair**—Use the drop-down menu to display the configured key pairs by name.
 - **Show**—Click to display information about the selected key pair, including date and time generated, usage (general or special purpose), modulus size, and key data.
 - **New**—Click to add a new key pair, providing a name, modulus size, and usage. When you generate the key pair, you have the option of sending it to the security appliance or saving it to a file.
- **Certificate Subject DN**—Identifies DN attributes for the certificate.
 - **Common Name (CN)**—Enter the FQDN or IP address of the security appliance.
 - **Organization (O)**—Provide the name of the company.
 - **Country (C)**—Enter the two-letter code for the country.
- **Optional Parameters**—Lets you add additional attributes for the signing request.
 - **Additional DN Attributes**—These include Department (OU), State (ST), Location (L), and E-mail Address (EA).
 - **FQDN (SubjectAlt Name)**—Use this certificate extension field to enter additional fully qualified domain name information if the CA requires it.
- **Generate Request**—Click to generate the certificate signing request, which you can then **Send** to Entrust, or **Save to File**, and send later.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Installing Identity Certificates

The **Install** button on the Identity Certificates window is inactivated unless there is a pending enrollment. Whenever the security appliance receives a Certificate Signing Request (CSR), the Identity Certificates window displays the pending ID certificate. When you highlight the pending Identity Certificate, the Install button activates.

When you transmit the pending file to a CA, the CA enrolls it and returns a certificate to the security appliance. Once you have the certificate, click the Install button and highlight the appropriate Identity and CA certificates to complete the operation.

The following steps illustrate adding and installing a pending Identity Certificate:

To Add the Identity Certificate:

-
- Step 1** In the **Identity Certificates** panel, click the **Add** button.
- Step 2** In the **Add Identity Certificate** panel, select **Add a new identity certificate**.
- Step 3** Optionally, change the key pair or create a new key pair. A key pair is required.
- Step 4** Enter the **Certificate Subject DN:** information and click the **Select...** button.
- Step 5** In the **Certificate Subject DN** panel, be sure to specify all of the subject DN attributes required by the CA involved. See [Certificate Subject DN Attributes](#). Then click **OK** to close the **Certificate Subject DN** panel.
- Step 6** In the **Add Identity Certificate** panel, click the **Advanced...** button.
- Step 7** In the **Advanced Options** panel, verify that the **FQDN:** field is the correct FQDN of the security appliance and click **OK** to close the window.
- Step 8** In the **Add Identity Certificate** panel, click the **Add Certificate** at the bottom.
- Step 9** When prompted to enter a name for the CSR, *specify an easily-accessible file name of type text, such as c:\verisign-csr.txt*.
- Step 10** Send the CSR text file to the CA. Alternatively, you can paste the text file into the CSR enrollment page on the CA's web site.

To install an Identity Certificate:

-
- Step 1** When the CA returns the Identity Certificate to you, return to the Identity Certificates panel, select the pending certificate entry, and click the now active **Install** button.
- Step 2** To assign the newly installed certificate for use with SSL VPN, navigate to the **SSL Settings** panel by SSL Settings hot link in the text under the list of certificates.
- Step 3** In the **SSL Settings** panel, double-click the interface to be assigned to the certificate. the **Edit SSL Certificate** panel opens.
- Step 4** In the **Edit SSL Certificate** panel, select the certificate from the **Certificate:** pull-down list and click **OK**. Note that the selected Identity Certificate displays in the **ID Certificate** field to the right of the selected **Interface** field.
- Step 5** Be sure to click the **Apply** button at the bottom of the **SSL Settings** panel to save the newly-installed certificate with the ASA configuration.

Code-Signer Certificates

Code signing appends a digital signature to the executable code itself. This digital signature provides enough information to authenticate the signer as well as to ensure that the code has not been subsequently modified since signed.

Code-signer certificates are special certificates whose associated private keys are used to create digital signatures. The certificates used to sign code are obtained from a CA, with the signed code itself revealing the certificate origin. You can import code-signer certificates with the **Import** button on this panel or you can select the Java Code Signer panel, Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Java Code Signer.

The Code-signer Certificate Authentication panel allows you to:

- Display details of an Identity Certificate. See [Show Code-Signer Certificate Details](#).

- Delete an existing Identity Certificate. See [Delete a Code-Signer Certificate](#).

Export an existing Identity Certificate. See [Import or Export a Code-Signer Certificate](#).

Show Code-Signer Certificate Details

The **Show Details** button displays the Code Signer Details dialog box, which shows the following information about the selected certificate:

- **General**—Displays the values for type, serial number, status, usage, public key type, CRL distribution point, the times within which the certificate is valid, and associated certificates. This applies to both available and pending status.
- **Issued to**—Displays the X.500 fields of the subject DN or certificate owner and their values. This applies only to available status.
- **Issued by**—Displays the X.500 fields of the entity granting the certificate. This applies only to available status.

Delete a Code-Signer Certificate

The **Delete** button immediately removes the selected Code Signer certificate configuration from the security appliance. Once you delete a configuration, it cannot be restored; to recreate the configuration, you must use the **Import** button to reenter the configuration information from the beginning



Note Once you delete a Code Signer configuration, it cannot be restored.

Import or Export a Code-Signer Certificate

Assign values to the fields in the **Import Certificate** window as follows:

- **Decryption Passphrase**: Specify the passphrase used to decrypt the PKCS12 file
- **Files to Import From**: You can type the pathname of the file in the box or you can click **Browse** and search for the file. **Browse** displays the **Import Certificate** dialog box, which lets you navigate to the file containing the certificate.

Assign values to the fields in the Export Certificate window as follows:

- **Export to file**—Specify the name of the PKCS12-format file to use in exporting the certificate configuration;
- Certificate Format: Click **PKCS12 format**, the public key cryptography standard, which can be base64 encoded or hexadecimal, or click **PEM format**.
 - **Browse**—Display the **Select a File** dialog box that lets you navigate to the file to which you want to export the certificate configuration.
- **Decryption Passphrase**—Specify the passphrase used to decrypt the PKCS12 file for export.
 - **Confirm Passphrase**—Verify the decryption passphrase.
- **Export Certificate**—Exports the configuration.

Local Certificate Authority

The Local Certificate Authority (CA) provides a secure configurable inhouse authority that resides the security appliance for certificate authentication.

**Note**

The local CA provides a certificate authority on the adaptive security appliance for use with SSL VPN connections, both browser- and client-based.

User enrollment is by browser webpage login. The Local CA integrates basic certificate authority functionality on the security appliance, deploys certificates, and provides secure revocation checking of issued certificates.

The following Local CA options allow you to initialize and set up the Local CA server and user database:

- Configure the Local CA Server on the security appliance. See [Configuring the Local CA Sever](#).
- Revoke/Unrevoke Local CA Certificates and update CRL. See [Manage User Certificates](#).
- Add, edit, and, delete Local CA users. See [Manage User Database](#).

Default Local CA Server

The Local CA window displays the parameters to be configured for setting up a Local CA Server on the security appliance. The default characteristics of the initial Local CA server are listed in the following:

Configurable Parameters

Enable/Disable buttons activate or deactivate the Local CA server.

The Enable passphrase secures the Local CA server from unauthorized or accidental shutdown

Certificate Issuer's Name

Issued certificate keypair size

Local CA Certificate key-pair size

Length of time the server certificate is valid

Length of time an issued user certificate

Simple Mail Transfer Protocol (SMTP) Server IP Address for Local CA e-mail

From-e-mail address that issues Local CA user certificate e-mail notices

Subject line in Local CA e-mail notices

More Options

Certificate Revocation List (CRL) Distribution Point (CDP), the location of the CRL on the Local CA security appliance

Length of time CRL is valid

Database Storage Location

Subject-name DN default to append to a username on issued certificates

Post-enrollment/renewal period for retrieving an issued certificate PKC12 file

Length of time a one-time password is valid

Days be expiration reminders are sent

Defaults

Default is disabled. Select Enable to activate the Local CA server.

Required - No default. Supply a word with a minimum of seven alphanumeric characters)

`cn=hostname.domainname`

1024 bits per key

1024 bits per key

Server Certificate=3 yrs.

User Certificate=1 yr.

Required - No default. You supply the SMTP mail server IP address.

Required - No default. Supply an e-mail address in `adminname@host.com` format.

"Certificate Enrollment Invitation"

More Defaults

Specify the location of the CRL on the Local CA security appliance,

`http://hostname.domain/+CSCOCA+/asa_ca.crl`

CRL =6 hrs.

On-board flash memory

Optional - No default. Supply a subject-name default value.

24 hours

72 hrs. (three days)

14 days prior to certificate expiration.

Configurable Parameters

Length of time a one-time password is valid

Defaults

72 hrs. (three days)

Caution: **Delete Certificate Authority Server** button permanently removes the server configuration.**Configuring the Local CA Server**

The CA Server window lets you customize, modify, and control Local CA server operation. This section describes the parameters that can be specified. Additional parameters are available when you click **More Options**. See [More Local CA Configuration Options](#). For permanent removal of a configured Local CA, see [Deleting the Local CA Server](#). To customize the Local CA server, first review the initial settings shown in the preceding table.

**Note**

Issuer-name and **keysize server** values cannot be changed once you enable the Local CA. Be sure to review all optional parameters carefully before you enable the configured Local CA.

Enable/Disable Buttons

The **Enable/Disable** buttons activate or deactivate the Local CA server. Once you enable the Local CA server with the **Enable** button, the security appliance generates the Local CA server certificate, key pair and necessary database files.

The self-signed certificate key usage extension has key encryption, key signature, CRL signing, and certificate signing ability. The **Enable** button also archives the Local CA server certificate and key pair to storage in a PKCS12 file.

**Note**

Click **Apply** to be sure you save the Local CA certificate and key pair so the configuration is not lost if you reboot the security appliance.

When you select the **Disable** button to halt the Local CA server, you shutdown its operation on the security appliance. The configuration and all associated files remain in storage. Webpage enrollment is disabled while you change or reconfigure the Local CA.

Passphrase

When you enable the Local CA Server for the first time, you must provide an alphanumeric Enable passphrase. The passphrase protects the Local CA certificate and the Local CA certificate key pair archived in storage. The passphrase is required to unlock the PKCS12 archive if the Local CA certificate or key pair is lost and needs to be restored.

**Note**

There is no default for the enable passphrase; the passphrase is a required argument for enabling the Local CA Server. Be sure to keep a record of the enable passphrase in a safe place.

Issuer Name

The Certificate Issuer Name field contains the issuer's subject name dn, formed using the *username* and the subject-name-default DN setting as `cn=<FQDN>`. The Local CA server is the entity granting the certificate. The default certificate name is provided in the format: `cn=hostname.domainname`.

CA Server Key Size

The CA Key Size parameter is the size of the used for the server certificate generated for the Local CA server. Key size can be 512, 768, 1024, or 2048 bits per key. The default size is 1024 bits per key.

Client Key Size

The Key Size field specifies the size of the key pair to be generated for each user certificate issued by the Local CA server. Key size can be 512, 768, 1024, or 2048 bits per key. The default size is 1024 bits per key.

CA Certificate Lifetime

The **CA Certificate Lifetime** field specifies the length of time in days that the CA server certificate is valid. The default for the CA Certificate is 3650 days (10 years).

The Local CA Server automatically generates a replacement CA certificate 30 days prior to the CA certificate expiration, allowing the replacement certificate to be exported and imported onto any other devices for Local CA certificate validation of user certificates issued by the Local CA certificate after expiration. The pre-expiration Syslog message:

```
%ASA-1-717049: Local CA Server certificate is due to expire in <days> days and a replacement certificate is available for export.
```



Note

When notified of this automatic rollover, the administrator must take action to ensure the new Local CA certificate is imported to all necessary devices prior to expiration.

Client Certificate Lifetime

The **Client Certificate Lifetime** field specifies the length of time in days that a user certificate issued by the CA server is valid. The default for the CA Certificate is 365 days (one year).

SMTP Server & Email Settings

To set up e-mail access for the Local CA server, you configure The Simple Mail Transfer Protocol (SMTP) e-mail server, the e-mail address from which to send e-mails to Local CA users, and you specify a standard subject line for Local CA e-mails.

- **Server IP Address** - The Server IP Address field requires the Local CA e-mail server's IP address. There is no default for the server IP address; you must supply the SMTP mail server IP address.
- **From Address** - The From Address field requires an e-mail address from which to send e-mails to Local CA users. Automatic e-mail messages carry one-time passwords to newly enrolled users and issue messages when certificates need to be renewed or updated. that issues Local CA user certificate e-mail notices. There is no From Address default value; you are required to supply an e-mail address in *adminname@host.com* format.
- **Subject** - The Subject field is a line of text specifying the subject line in all e-mails send to users by the Local CA server. If you do not specify a subject field, the default inserted by the Local CA server is "Certificate Enrollment Invitation".

More Local CA Configuration Options

CRL Distribution Point URL

The Certificate Revocation List (CRL) Distribution Point (CDP) is the location of the CRL on the security appliance. The default CRL DP location is `http://hostname.domain/+CSCOCA+/asa_ca.crl`.

Publish CRL Interface and Port:

To make the CRL available for HTTP download on a given interface or port. Select an interface from the pull-down list. The optional port option can be any port number in a range of 1-65535. TCP port 80 is the HTTP default port number.

The CDP URL can be configured to utilize the IP address of an interface, and the path of the CDP URL and the file name can be configured also. (Note that you cannot rename the CRL; it always has the fixed name, LOCAL-CA-SERVER.crl.)

For example, the CDP URL could be configured to be: `http://10.10.10.100/user8/my_crl_file` In this case only the interface with that IP address works, and, when the request comes in, the security appliance matches the path `/user8/my_crl_file` to the configured CDP URL. When the path matches, the security appliance returns the CRL file stored in storage. Note that the protocol must be `http`, so the prefix is `http://`.

CRL Lifetime

The Certificate Revocation List (CRL) Lifetime field specifies the length of time in hours that the CRL is valid. The default for the CA Certificate is six hours.

The Local CA updates and reissues the CRL every time a user certificate is revoked or unrevoked, but if there are no revocation changes, the CRL is reissued once every CRL lifetime. You can force an immediate CRL update and list regeneration with the **CRL Issue** button on the Manage CA Certificates panel.

Database Storage Location

The Database Storage Location field allows you to specify a storage area for the Local CA configuration and data files. The security appliance accesses and implements user information, issued certificates, revocation lists, and so forth using a Local CA database.

That Local CA database resides can be configured to be on an off-box file system that is mounted and accessible to the security appliance. To specify an external file or share, enter the pathname to the external file or click **Browse** and search for the file.



Note Flash memory can store a database with 3500 users or less, but a database of more than 3500 users requires off-box storage.

Default Subject Name

The Default Subject Name (DN) field allows you to specify a default subject name to append to a username on issued certificates. The permitted DN attribute keywords are listed in the following list:

Default Subject-name-default DN Keywords
CN= Common Name
SN = Surname
O = Organization Name
L = Locality
C = Country
OU = Organization Unit
EA = E-mail Address

Default Subject-name-default DN Keywords

ST = State/Province

T = Title

Enrollment Period

The Enrollment Period field specifies the number of hours an enrolled user can retrieve a PKCS12 enrollment file in order to enroll and retrieve a user certificate. The enrollment period is independent of the OTP expiration period. The default Enrollment Period is 24 hours.



Note Certificate enrollment for the Local CA is supported only for Clientless SSL VPN connections and is not supported for other SSL VPN clients such as CVC or for IPSec VPN connections. For clientless SSL VPN connections, communications between the client and the head-end is through a web browser utilizing standard HTML.

One-Time-Password Expiration

The One-Time-Password (OTP) expiration field specifies the length of time that a one-time password e-mailed to an enrolling user is valid. The default value is 72 hours.

Certificate Expiration Reminder

The Certificate Expiration Reminder field specifies the number of days before expiration reminders are sent to e-mailed to users. The default is 14 days.

Apply Button

The **Apply** button lets you save the new or modified CA certificate configuration.

Reset Button

The **Reset** button removes any changes or edits and returns the display to the original contents.

Deleting the Local CA Server

The **Delete Certificate Authority Server** button at the bottom of the **More Options** section of the **CA Server** panel, immediately removes the Local CA Certificate configuration from the security appliance. Once you delete the Local CA configuration, it cannot be restored; to recreate the deleted configuration, you must reenter the certificate configuration information from the beginning.



Note Deleting the Local CA Server removes the configuration from the security appliance. Once deleted, the configuration is unrecoverable.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	—	•	—	—

Manage User Certificates

The Local CA server maintains certificate renewals, re-issues user certificates, maintains the Certificate Revocation List (CRL), and revokes or restores privileges as needed. With the Manage User Certificates window, you can select specific certificates by username or by certificate serial number and change the certificate status (revoked/unrevoked).

Whenever you change any certificate status, be sure to update the CRL to reflect the latest changes.

- To change certificate status, see [Revoking a Local CA Certificate](#) and [Unrevoking a Local CA Certificate](#).

Revoking a Local CA Certificate

The Local CA Server keeps track of the lifetime of every user certificate and e-mails renewal notices when they are needed. If a user's certificate lifetime period runs out, that user's access is revoked. The Local CA also marks the certificate as revoked in the certificate database and automatically updates the information and reissues the CRL.

Unrevoking a Local CA Certificate

An already revoked user certificate can have privileges restored with notification by e-mail. Select a revoked user's certificate and click Unrevoke to restore access. The Local CA also marks the certificate as unrevoked in the certificate database, automatically updates the certificate information, and reissues an updated CRL.

Manage User Database

The Local CA user database contains user identification information and the status of each user in the system (enrolled, allowed, revoked, etc.). With the Manage User Database window, you can add new users, select specific users by username to edit user information, and you can delete existing users and their certificates. Whenever you add a user or modify any user's status, The Local CA automatically updates the CRL to reflect the latest changes.

- To add a user to the Local CA Database, see [Add a Local CA User](#).
- To change user identification information for an existing user, see [Edit a Local CA User](#).
- To remove a user from the database, see [Delete a Local CA User](#).
- To change the enrollment status of a user, see [Allow Enrollment](#).
- To e-mail One-Time-Passwords (OTPs) to a user, see [Email OTP](#).
- To view or regenerate a OTP, see [View/Re-generate OTP](#).

Add a Local CA User

The **Add** button allows you to enter a new user into the Local CA database. Each new user to be entered into the database must have a predefined user name, e-mail address, and subject name. **Local CA Add User Fields**

- Username: Enter a valid user name.
- Email: Specify an existing valid e-mail address.
- Subject: Enter the user's subject name.

Email OTP

The **Email OTP** button automatically sends an e-mail notice of enrollment permission with a unique one-time password (OTP) and the Local CA enrollment webpage URL to the newly added user.

Replace OTP

The **Replace OTP** button automatically reissues a new one-time password and sends an e-mail notice with the new password to the newly added user.

Edit a Local CA User

The **Edit** button allows you to modify information on an existing Local CA user in the database. Select the specific user and click the **Edit** button.

You can modify the same fields as with the [Add a Local CA User](#) button. You can e-mail a new or replacement OTP to the user. Existing user information that can be modified includes user name, e-mail address, and subject name.

Delete a Local CA User

The **Delete** button removes the selected user from the database and removes any certificates issued to that user from the Local CA Database. A deleted user cannot be restored; to recreate the deleted user record, you must use the **Add** button to reenter the user information.

Allow Enrollment

The **Allow Enrollment** button enrolls the selected user.

Email OTP

The **Email OTP** button sends an OTP to the selected user by email.

View/Re-generate OTP

The **View/Re-generate OTP** button launches a window where you can regenerate the OTP of the selected user.

